International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 179-186

TRANS STELLAR
• Journal Publications • Research Consultancy

DETECTING ATTACKS AND PREVENT STATIC AND DYNAMIC WEBSITES FROM THOSE TYPES OF ATTACK

N. A. PAWAR & Y. C. KULKARNI

Information Technology, Bharati Vidyapeeth Deemed University, Pune, Maharastra, India

ABSTRACT

In today's life internet plays important role. All applications and services have made human life very easy. It can be use from basic level to higher level of communication and managing any personal information. In applications, data is increased and complexity of that data is also increased. To resolve this problem multitier web server can be used. There is rapid increase in globalization and use of internet is also increased. In previous multitier websites to prevent the attacks, different IDS can be used for static and dynamic websites. In our paper we use same IDS for static as well as dynamic website. Although newly search attacks and their prevention can also explain in this paper.

KEYWORDS: False Positive, Intrusion Detection System, Penetrator, Signature, Vulnerabilities

INTRODUCTION

There are different tasks such as banking; communication & travelling are carried out through web. All these web services are carried through web server front end and back end server. Front end runs the application user interface logic and back end server consist database and file server. Due to large database contain in web server it can be attacked by many attacker. Recently these attacks are multiform that can be attack to the front end by finding vulnerabilities [6], [5], [1]. Firewall can be used to protect database server, while web server can be easily accessible by internet. IDS system gives solution on this problem. IDS system protects multitier web services by matching misused traffic patterns or signatures [20], [3], [18], [2].

To strengthen the system & to protect against internal and external attack IDS have been widely used. Anomaly detection and misused detection are two techniques through which IDS can detect the intrusion in the system.

In Anomaly detection technique there is difference in user normal activity which can be consider as an anomalous behavior. In misused detection previous pattern can be matched to the current system attacks called as "signature". Historically, IDS used for auditing system information but the main need for IDS was to log the files in the system that was not processed by human.

Latest IDS implement advanced and smart system which handling complexity of intrusions and huge amount of data. When any privilege user can attack to the web server in that case both the database IDS and web server IDS cannot differentiate where that user is credential or not. Neither web server IDS nor database IDS find out this type of attack. Mapping between database server and web server is not feasible in multithreaded web server architecture.

In the existing system we require different IDS for different web sites. For Static website required different IDS and for dynamic website required different IDS. So it needs to create different IDS each time according to the website. In this paper we are implementing "Double Guard" that handle both sides of attack. Attack may be from static web site or attack may be from dynamic web site. No need to create two different IDS for two different web sites. Double Guard can

handle both types of attack. There are different types of attacks like privilege escalation attack, hijack future session attack, injection attack, direct database attack all these attacks are present in our previous system. We search some new attacks that can cause damage to our multitier web service, like session fixation attack, input validation attack, brute force attack and prevention measures to protect all these types of attacks.

We use virtualization technique for assigning each user session with dedicated container, so that there is direct mapping between web server and database queries can be happen. We have implemented our Double Guard container architecture using DOT NET framework .We use ephemeral containers that can be easily instantiated and easily destroyed. We assigned each client session a dedicated container so that, when attacker attack to any session its result cannot affected to another sessions.

In this paper we use two websites, first website is static type and another one is dynamic website. In static website back-end data cannot change while in dynamic website back-end data will be always modified. Dynamic websites contain HTTP requests include back end queries. To avoid leakage of data in these websites we use Double Guard to protect our system using IDS and provide prevention measures on it.

LITERATURE STUDY

Intrusion Detection System provides security of web servers to identify malicious activity and to provide response to attacks. Using simple pattern matching techniques to the HTTP content detection of attacks has been performed. IDS are identifying one or more input streams .previously IDS has two approaches: first is Anomaly detection or second is misuse detection. Anomaly detection depends on users, the applications, or the network. An anomaly detector then compares actual usage patterns with established profile to identify abnormal patterns. Second approach is misuse detection contain number of attacks description. There is big difference between anomaly detection and misuse detection is that, in anomaly detection it detected previously unknown attacks.

While in misuse detection it can detect attacks that have been modeled. In anomaly detection large number of false positive rate is present which is contrast in misuse detection contain less prone false positive rate. Depending upon type of analysis misuse detection system can be classified as a stateful analysis or stateless analysis.

In statless analysis each event in the input stream examines independently while in stateful analysis there is relationship between events occur and it recognizes the attack histories. Stateful analysis is more powerful than stateless analysis to detect complex attacks. Misuse detection of web based has been performed at network level and at the application level [16]. In network level it control network traffic while in application level it access server logs [7]. IDS cannot consider application level logic that's the reason it cannot identify attacks of organization of server application.

There are two groups that attack computer system. They are external penetrators and internal penetrator. External penetrators are unauthorized user of the system. Internal penetrators are authorized user of the system. Internal penetrators can be divided into groups.

- **Clandestine Users:** They hide system mechanism.
- **Misfeasors:** These are authenticate user that performs misuse of another.
- **Masqueraders:** They are privilege user.

The main work of intrusion related alert is to transform intrusion detection sensor alert into intrusion report to avoid replication of intrusion alerts [12]. IDS uses information to detect intrusions. Because of large information contain in database it should receive highest level of protection. This is reason that significant research can be made on IDS database [4], [9], [15] and IDS firewalls [21]. Intrusions and vulnerabilities have been detected and analyzing the source code or executables [13],[8],[19]. The new container-based web server architecture in Double guard separate the information flows by each session. This indicates that information flow from the web server to the database server for each session. In static web page, our Double Guard approach does not require application logic for building a model. For dynamic web services, there is no need of application logic.

Intrusions can be detected by IDS in two ways, like active and passive, in active type IDS take some actions to detect intrusions. In passive attack IDS shows an alarm and notifications .Another characteristic of IDS is its tendencies of intrusion detection system, the way that IDS can be arrange. IDS can be centralized means it is having only one module. In distributed IDS entities are distributed over network. Intrusion detection and prevention contains two types of errors which are false positives and false negatives. In false positive lawful actions considered as malicious so that errors are blocked. In false negatives malicious actions of errors not detected currently. One limitation of IDS is that it does not detect attacks that exploit the logic errors; one example of it is that any program that fails to check its authentication before begins it.

CLAMP [10] is architecture to protect the data even in the presence of attacks. In CLAMP user sensitive data can accessed for different user by separated code between web servers and database servers. Whereas, Double Guard doing its job by mapping patterns between HTTP requests and DB queries to detect infected user sessions. CLAMP requires modification to the existing application code, and the Query Restrictor works as a proxy to manage all database access requests. Double Guard need process isolation on another hand CLAMP requires platform virtualization, and CLAMP contain more isolation than Double Guard. CLAMP can be effective in detecting attacks than Double Guard because of its good isolation. For Building the mapping model in Double Guard would require a large number of isolated web stack instances so that mapping patterns would distributed across different session instances.

Virtualization is used to improve security and to isolate objects performance. In virtualization Full virtualization and Para-virtualization are approaches being taken. Lightweight virtualization, such as OpenVZ [14], Parallels Virtuozzo [17], or Linux-V Server [11], are based on some sort of container concept. In containers, a group of processes always have its own dedicated system, though it is running in an isolated environment. Lightweight containers can have measurable performance. Single physical host can run Thousands of containers. In our Double Guard, we used the container ID to separate session traffic for mapping relationships between web server requests and database query events.

SYSTEM ARCHITECTURE

We initially set up our threat model to include our assumptions and the types of attacks we are aiming to protect and preventions measures to prohibit these attacks. We assume that both the web and the database servers have its vulnerability. Attacks are come from the web clients. Any attack first attack the application logic of the system then attacks its web server. Using web server the attackers can attack the database server. The current IDS cannot detect attacks made on web server and database server. It is easy to attack on web server than the database server. Data present on the web server it can be publically available to everyone rather than the data which one available on database is not seen to everyone. When attacker attack on web server they get modified data present over application logic. It is difficult in case of

database server .When attacker wants to attack on database server the data cannot bypass directly. Attacker hijacks data in database server directly by submitting SQL queries.

ARCHITECTURE & CONFINEMENT

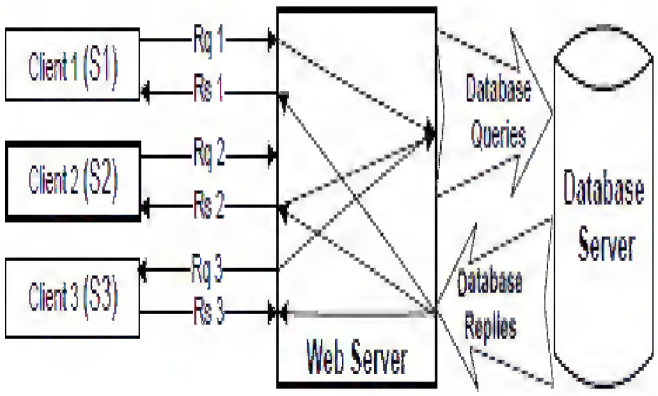

Figure 1: 3-Tier Model

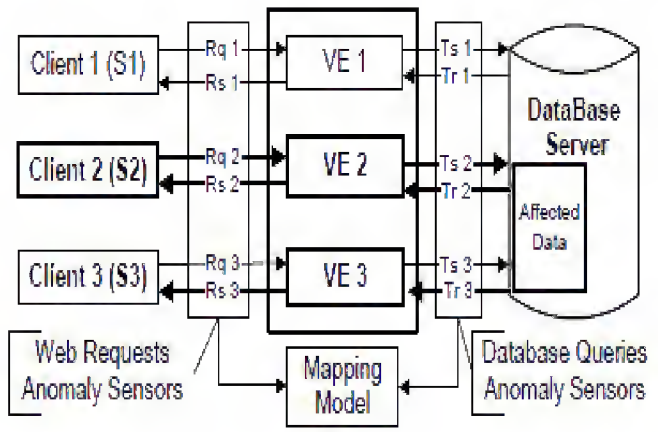

Figure 2: Web Server Instances Running in Containers

All network traffic, from both authenticates users and attacker, is entering then intermixed at the same web server. If an attacker committed to web server then this attacker access all its sessions. If we assign each session to a web server then it is not right as it will reduce all resources of web server. Many containers, runs A single physical web server each server is an exact copy of the original web server. Considering, from a logical perspective, each session is isolated from other sessions. We use separate communications at the session level so that a single user always deals with the same web server. In Session, there are different users, and we made the Communication of a single user to the same web server, to identify doubtful behavior by both session and user. In a session, if we detect abnormal behavior it will treat all traffic within this session as tainted.

Figure 1 define classic 3-tier model. The model is consist of 3 content .first is client or user .second is of web server. Third is of database server. In this model it is difficult to predicate which database corresponds to their respective web server. Relation among database and web server is difficult to understand.

Figure 2 resolve the problem which is occurred in previous figure. In this figure shows there is good mapping between database and client. Each session is individually connected to the web server. Each session will be isolated from other so that intrusions can not affect whole sessions from web server.

NEED OF IDS

Before DoubleGuard was developed the system which is present prevents web server and database from Linerization attack only.Before doubleguard not much security provided to the web server and database.This system can not handle all attack.we need to use 2 different technology, one for web server and another for database to prevent from attacks. In the proposed system we are prevent our web server and database from all types of attacks that exsiting system does not prevent.

EXISTING ATTACK

Following types of attacks on web server and database can not be handled in existing system

Privilege Escalation Attack

It is too hard to our security expert to protect our network from hackers. In this attack hackers can use to gain unauthorized access to network. It can hack the privilege of another user to get their data. There are two types of Privilege Escalation Attack .one is horizontal escalation and another is vertical escalation. Privilege means it is security of program. In horizontal escalation attacker can access information of another user. Accessing username and password is a best example of horizontal escalation. On other hand to hack data using vertical escalation is very difficult. Attacker can use ladder of privileges while using vertical escalation. The best example of it is bypass lock screen of today's Smartphone. In privilege escalation attack user can access data, deleting files and changing code without permission of user

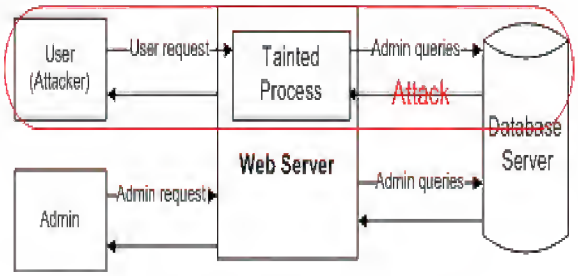

Figure 3: Privilege Escalation Attack

Hijack Future Session Attack

This attack is carried out at web server side.all sessions can be hijacks when attack can be made.By hijacking other user sessions,attacker not response to any request and send fake replies to the user.This attack classified as spoofing/Man-in the middle attack,a denial-of –service attack.In this attack web server can harm all sessions by not generating any database queries from normal user request.both web server IDS and database IDS cannot detect such attacks.to prevent this attack we use isolated container so that attacker cannot harm the sessions.

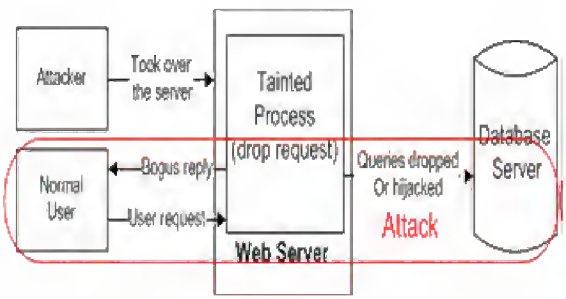

Figure 4: Hijack Future Session Attack

Injection Attack

In SQL injection attacks the attacker doesn't required to take help of web server. Attacker use the vulnerabilities present in the web server logic using that vulnerability attacker made out attack in the back end of database. It changes the structure of original SQL queries to exploit attacks into them. To avoid this type of attack the SQL query that exploit may change its behaviour when it goes through web server to detect attacker code.

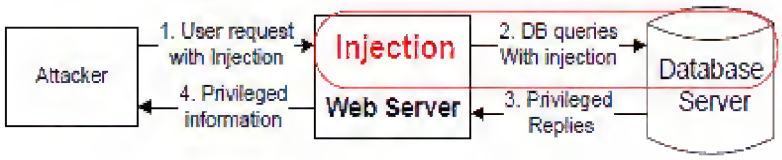

Figure 5: Injection Attack

Direct DB Attack

Any attacker attack database directly without passing through web server or its firewalls.Attacker in direct database attack take over the web server and sending queries to database server without sending web request o web server.neither web server IDS nor database IDS can detect this attack.Due to valuable data contain in database this attack affect broad change in the whole system.

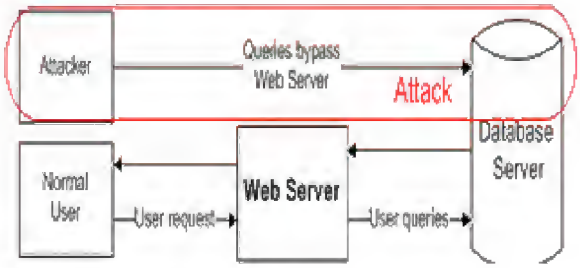

Figure 6: Direct DB Attack

PROPOSED ATTACKS

Input Validation Attack

The root cause of most attacks is input validation attack.In this attack all the inputs thats received to the web server should be considered as valid.all these inputs are data types,data ranges,buffer sizes and metacharacters.The attack is made by attacker to bypass the javascript.To avoid this attack we notify the attacker that without enabling javascript he/she cannot login to that page .

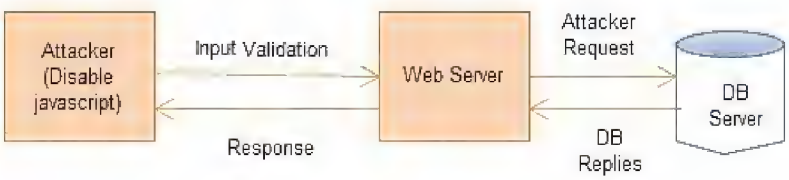

Figure 7: Input Validation Attack

Brute Force Attack

Continuous trying list of different passwords,words or letters do not decrypt any information. In brute force attack attacker continueously used guessed password or words until it gain access of account of other user.A brute force attack

involves trying every key combination to find the correct password that will hack an account of another user.Due to different combinations of symbols,words or numbers it will reqiured more time to the attacker to attack.The time required to occured this attack is depends on complexity of password,strength of encryption,strength of computer being used and how well attacker used target.To prevent this attack developer can make system such a way that after certain attempt the account will lock automatically.

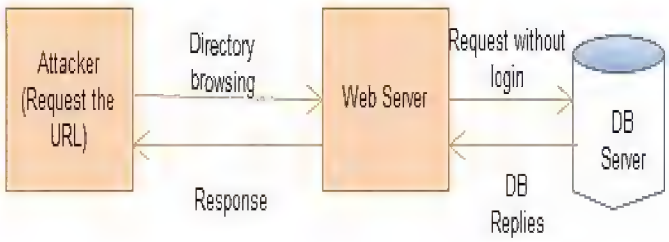

Figure 8: Brute Force Attack

CONCLUSIONS

We presented in multi-tiered web applications an intrusion detection system that builds models for both front-end web (HTTP) requests and back-end database (SQL) queries. We built up the model of static and dynamic web requests with the back-end file system and database queries. Attacks that are occurred at static as well as dynamic websites we show that attacks. Same IDS can be used for static as well as dynamic websites. In our previous paper we used OpenVZ instead of that we use IIS here. By using minimal false positive Intrusion Detection System detects attacks.

ACKNOWLEDGMENTS

The authors would like thanks to the publishers, researchers for making their resources available and teachers for their guidance. We would also thank the college authority for providing the required infrastructure and support. Finally we would like to give a heart fully gratitude to friends and family members.

REFERENCES

1. http://www.sans.org/top-cyber-security-risks/.
2. B. I. A. Barry and H. A. Chan. Syntax, and semantics-based signature database for hybrid intrusion detection systems. Security and Communication Networks, 2(6), 2009.
3. H.-A. Kim and B. Karp. Autograph: Toward Automated, worm signature detection. In USENIX Security Symposium, 2004.
4. Lee, Low, and Wong. Learning fingerprints for a database intrusion detection system. In ESORICS: European Symposium on Research in Computer Security. LNCS, Springer-Verlag, 2002.
5. Common vulnerabilities and exposures. http://www.symantec.
6. Five common web application vulnerabilities.. com/connect/articles/five-common-web-application-vulnera bilities.
7. R. Fielding. wwwstat: HTTP d Log file Analysis Software. http://ftp.ics.uci.edu/pub/websoft/wwwstat/, November 1996.

8. M. Christodorescu and S. Jha. Static analysis of executables to detect malicious patterns.
9. Y. Hu and B. Panda. A data mining approach for database intrusion detection. In H. Haddad, A. Omicini, R. L. Wainwright, and L. M. Liebrock, editors, SAC. ACM, 2004.
10. B. Parno, J. M. McCune, D. Wendlandt, D. G.Andersen, and A. Perrig. CLAMP: Practical prevention of large-scale data leaks.In IEEE Symposium on Security and Privacy. IEEE Computer Society, 2009.
11. Linux-vserver. http://linux-vserver.org/.
12. F. Valeur, G. Vigna, C. Kr¨ugel, and R. A. Kemmerer. A comprehensive approach to intrusion detection alert correlation. IEEE Trans. Dependable Sec. omput, 1(3), 2004.
13. D. Wagner and D. Dean. Intrusion detection via static analysis. In Symposium on Security and Privacy (SSP'01), May 2001.
14. Openvz. http://wiki.openvz.org.
15. A. Srivastava, S. Sural, and A. K. Majumdar. Database intrusion detection using weighted sequence mining.JCP, 1(4), 2006.
16. M. Roesch. Snort - Lightweight Intrusion Detection for Networks. In Proceedings of the USENIX LISA' 99 Conference, November 1999.
17. Virtuozzo containers.http://www.parallels.com/products/pvc45/.
18. Liang and Sekar. Fast and automated generation of attack signatures: A basis for building self-protecting servers. In SIGSAC: 12th ACM Conference on Computer and Communications Security, 2005.
19. V. Felmetsger, L. Cavedon, C. Kruegel, and G. Vigna.Toward Automated Detection of Logic Vulnerabilities in Web Applications. In Proceedings of the USENIX Security Symposium, 2010.
20. J. Newsome, B. Karp, and D. X. Song. Polygraph: Automatically generating signatures for polymorphic worms. In IEEE Symposium on Security and Privacy. IEEE Computer Society, 2005.
21. K. Bai, H. Wang, and P. Liu. Towards database firewalls. In DBSec2005.

AUTHOR DETAILS

Ms. Nayana. A. Pawar received a B.E. (Comp. and Sci.) in 2009 from Shivaji University. I am pursuing a Master Degree in Information Technology from Deemed University B.V.D.U .C.O.E. Pune 46. My interest and research area is Computer security.